

DOTTIE TOTS NURSERY SCHOOL

Online Safety, Mobile Phones, Cameras and Electronic Devices Policy



Document reference	DT-P-01.6
Document type	Policy
Revision	A - August 2026
Effective date	1 September 2026
Owner / approver	Leadership and Management Team
Next review	August 2027, or sooner following a safeguarding, technology, legal or operational change

CORE SAFEGUARDING RULE

Personal devices must not be used to photograph, film or record children. Images, recordings and children's information may be created, accessed and shared only for an authorised purpose, on approved systems and under DT safeguarding, privacy and security controls.

1. Policy statement

Dottie Tots Nursery School safeguards children from online harm, inappropriate content, unauthorised photography or recording, data loss and unsafe use of connected technology. Digital tools support communication and administration only where their use is lawful, proportionate, secure and does not reduce supervision or responsive interaction with children.

This policy applies at Bentley and Kingsley, on outings, during home working with DT information, at events and whenever a person is acting for Dottie Tots.

2. Scope and definitions

- It applies to employees, agency staff, volunteers, students, contractors, visiting professionals, parents, carers and other visitors.
- Devices include phones, tablets, laptops, cameras, wearable devices, smart watches, gaming devices, storage media and any equipment capable of imaging, recording, communication or sharing.
- Online safety includes harmful or inappropriate content, contact, conduct and commercial risks, grooming, exploitation, cyber-bullying, misinformation, privacy breaches and unsafe data sharing.
- This policy governs safeguarding and device controls. DT-P-07.2 governs whether and how children use screens for learning, development, communication or wellbeing.

3. Legal and statutory framework

- Early Years Foundation Stage statutory framework for group and school-based providers, effective 1 September 2026, including safeguarding, supervision, privacy, information handling and personal-device requirements.
- Children Act 1989 and Children Act 2004; Working Together to Safeguard Children; and Hampshire Safeguarding Children Partnership procedures.
- Data Protection Act 2018 and UK GDPR; Protection of Children Act 1978; Sexual Offences Act 2003; Computer Misuse Act 1990; Online Safety Act 2023; Equality Act 2010 and Human Rights Act 1998.

4. Approved equipment, accounts and access

- Only DT-approved devices, accounts, applications and storage locations are used for children's information, images, recordings, observations or parent communication.
- Devices are password or passcode protected, locked when unattended, updated, protected against malware where applicable and accessible only to authorised users.
- Passwords are individual, not shared informally, and changed immediately following suspected compromise or a role/access change.
- Access follows least-privilege principles. Leavers and people changing role have access removed promptly.
- Children's information is not copied to personal email, personal cloud storage, removable media or unapproved messaging services.
- The Nursery Manager maintains a device and authorised-user record and ensures faults, loss or compromise are reported immediately.

5. Personal mobile phones and personal devices

- Staff, volunteers and students store personal phones and devices in the designated secure place before working with children. They are not carried on the person in childcare, sleep, toileting or changing areas.
- Personal devices are used only during an authorised break in a child-free area. Emergency use requires the Nursery Manager's permission and must not expose children or confidential information.
- On outings, a personal phone may be authorised solely as an emergency communication device where DT equipment is unavailable. It must not be used to photograph or record children and the risk assessment records the control.
- Smart watches and wearable devices with imaging, recording, messaging or internet functions are switched off or placed in the designated secure storage unless a documented reasonable adjustment has been agreed with equivalent safeguards.
- Staff do not access personal email, social media, messaging, calls or entertainment while supervising children.

6. Visitors, parents, contractors and visiting practitioners

- Visitors are told the device rules on arrival and keep devices stored or unused in childcare areas unless use is expressly authorised and supervised.
- A contractor or lone worker who must maintain contact with an employer is directed to a child-free area or follows a written, supervised arrangement.
- A visiting practitioner may use an approved or declared device to play audio only after authorisation; it remains supervised and cannot be used to image, record or access information about children.
- Parents and visitors do not photograph, film or livestream in the setting unless DT has authorised a specific event arrangement. Permission to photograph one's own child does not permit capturing or publishing another child, staff member or confidential information.
- Suspected covert recording or unauthorised device use is challenged where safe, reported immediately and managed as a safeguarding and information-security concern.

7. Children's devices

- Parents are asked not to send children with personal phones, smart watches, cameras or connected toys.
- Where a device is needed for medical, communication, disability or other individual reasons, the Nursery Manager and SENCO agree a written risk-managed arrangement with the family.
- An unexpected device is switched off where practicable, securely stored, recorded and returned directly to the parent or carer. Staff do not search content unless authorised under a safeguarding response and lawful procedure.

8. Images, video and audio recordings

- Written parental permissions are obtained and recorded, but consent does not replace DT's duty to establish a lawful, necessary and proportionate purpose.
- Only the minimum images or recordings needed are taken. Routine assessment relies principally on practitioner observation and professional judgement.
- Children are treated with dignity: no image is taken during intimate care, toileting, changing or in a state of undress, distress or compromised dignity.

- Images are reviewed before sharing so they do not reveal another child, sensitive information, location data, documents, displays or unsafe practice.
- Images and recordings are shared only through the approved secure system with authorised recipients and are retained and deleted under DT's retention arrangements.
- Publicity use requires the applicable permission and risk assessment. A child is not identified by full name alongside an image and unnecessary location or uniform identifiers are avoided.
- A child who indicates they do not wish to be photographed or recorded is listened to, even where parental permission exists, unless recording is necessary to protect life or evidence a safeguarding incident.

9. Internet access, filtering and content

- Children never have unsupervised internet access. Any child-facing access is purposeful, brief, directly co-engaged by an adult and governed by DT-P-07.2.
- Filtering, safe-search and device restrictions are enabled and checked. These controls support but never replace adult supervision and pre-checking of content.
- Staff pre-view links, videos and resources. Autoplay, algorithmic feeds, adverts, comments, live chat and open search are disabled or avoided.
- Unexpected harmful content is removed from view immediately; staff reassure children, preserve relevant details without further dissemination, and report to the DSL.
- Illegal child sexual abuse material is not downloaded, copied, forwarded or investigated by staff. Concerns are reported urgently through safeguarding and police/CEOP routes; public online material may be reported to the Internet Watch Foundation as appropriate.

10. Social media, messaging and professional boundaries

- Staff use approved DT channels for work communication and maintain professional boundaries online.
- Staff do not accept or initiate social-media connections with current children and do not use personal accounts to communicate with children or families about nursery business.
- No confidential, identifying, disparaging or workplace-sensitive information is posted. Naming Dottie Tots in a personal profile does not authorise speaking for the organisation.
- Staff report online contact, content or behaviour that may place a child, colleague or the organisation at risk. Concerns about an adult's conduct follow DT-PR-01.1A.

11. Online safeguarding education and response

- Children learn simple, age-appropriate messages: use technology with a trusted adult; be kind; keep personal information safe; stop and tell an adult if something worries or confuses them.
- Online harm, grooming, exploitation, radicalisation, sexualised content, cyber-bullying or unsafe adult contact is treated as a safeguarding concern and reported immediately to the DSL/DDSL.
- The DSL follows Hampshire thresholds and referral routes and considers children's social care, police, CEOP, LADO and Ofsted duties according to the circumstances.
- The child is supported without blame, leading questions or promises of secrecy. Accurate contemporaneous records are secured in the safeguarding system.

12. Loss, breach or cyber incident

1. Report a lost device, mistaken disclosure, suspicious message, unauthorised access or other breach to the Nursery Manager immediately; do not conceal, delete or independently investigate it.
2. Take safe containment action, such as disconnecting a device, recalling a message where available or changing compromised credentials, without destroying evidence.
3. Inform the Head of Operations and Company Director/DSO promptly and assess safeguarding, data-protection, police, insurer and other notification requirements.
4. Record what happened, information and people affected, containment, advice, notifications, communication, recovery and lessons learned.

13. Roles and responsibilities

Role	Responsibility
Company Director / Ofsted Nominated Person / DSO	Retains complete strategic and safeguarding oversight, approves policy, receives material concerns and ensures consistent implementation across Bentley and Kingsley.
Head of Operations	Coordinates operational implementation, resources, audits and cross-setting follow-up, while keeping the Company Director fully informed.
Nursery Manager / DSL	Leads setting implementation, authorises practice, checks compliance, manages concerns and reports to the Head of Operations and Company Director/DSO.
Deputy Manager / DDSL	Acts in the Manager/DSL's absence, supports monitoring and escalates concerns without delay.
All staff, students and volunteers	Follow this policy, maintain active supervision and report any concern, breach or uncertainty immediately.

14. Training, monitoring and records

- Device rules, online safety, image handling, breaches and reporting routes form part of induction and are reinforced through supervision and staff meetings.
- The Nursery Manager checks storage arrangements, authorised devices, access permissions, image use and compliance in practice; the Head of Operations audits implementation across settings.
- Records include permissions, device/asset lists, authorised access, risk assessments, training, incidents, breaches, decisions, notifications and corrective actions.
- Any exception or reasonable adjustment is written, time-limited, risk assessed and authorised, with the Company Director retaining oversight of material decisions.

15. Related documents

- DT-P-01.1 Child Protection and Safeguarding Policy; DT-PR-01.1A Managing Allegations, Low-Level Concerns and LADO Procedure; DT-PR-01.1B Ofsted Notifications and Significant Events Procedure.
- DT-P-07.2 Screen Use and Digital Technology Policy; SEND Policy; Staff Code of Conduct; Data Protection and Confidentiality policies; Records Retention arrangements.

16. Sources and review

- EYFS statutory framework for group and school-based providers, effective 1 September 2026: <https://www.gov.uk/government/publications/early-years-foundation-stage-framework--2>
- DfE Help for early years providers - Internet safety and Screen use: <https://help-for-early-years-providers.education.gov.uk/>
- Hampshire Safeguarding Children Partnership procedures: <https://hipsprocedures.org.uk/>
- National Cyber Security Centre guidance for early years settings: <https://www.ncsc.gov.uk/guidance/early-years-practitioners-using-cyber-security-to-protect-your-settings>

This policy is reviewed annually and sooner following an incident, audit finding, inspection outcome or relevant change. The Company Director/Ofsted Nominated Person/DSO retains complete oversight of the review and any material exception.

Appendix 1 - Staff acknowledgement

I confirm that I have read and understood this policy. I will follow DT device, image, recording, online-safety, confidentiality and reporting controls and will report any concern, breach or uncertainty immediately.

Name	Role	Signature	Date

Document: DT-P-01.6 - Online Safety, Mobile Phones, Cameras and Electronic Devices Policy